

Notice of Allowability

Application No.

10/611,635

Examiner

Samson B. Lemma

Applicant(s)

AARON, JEFFREY A.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed on 09/13/2007.
2. ☒ The allowed claim(s) is/are 1,3,6,8,10-26,28-38,41-43 and 45-53.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 09/06/2007.
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. This is in reply to amendment after non-final office action, filed on September 11, 2007. **Claims 2, 4-5, 7, 9, 27, 39-40 and 44** are canceled. Thus claims **1, 3, 6, 8, 10-26, 28-38, 41-43 and 45-53** are pending/examined.
2. There **are six independent claims** namely **1, 16, 31, 48, 50 and 52**. **All the claims, including each independent claim are amended except dependent claims 20, 22, 24-26 and 28-29.**
3. Applicant's representatives, Jodi L. Hartman Reg. No. 55,251, and Examiner have conducted a telephone interview on September 6, 2007. During the interview, Independent claims were discussed. Furthermore the parties discussed how the claims should be amended at least to overcome the ground of rejection set forth in the pervious office action. However, during the discussion, Applicant's representative has been informed that further search/consideration and approval from the supervisor is needed before the claims are allowed.

Allowable Subject Matter

4. **Claims 1, 3, 6, 8, 10-26, 28-38, 41-43 and 45-53** are allowed.
5. The following is an examiner's statement of reasons for allowance:
6. **Claims 1, 3, 6, 8, 10-26, 28-38, 41-43 and 45-53** are allowed for the following reasons.

Referring to the **Independent claims 1, 16, 31**, the references on the record namely **Cisco**, discloses each and every limitations recited in the previous independent claims 1, 16 and 31 before the claims were amended.

For instance, referring to the previous independent 1, 16 and

31 Cisco discloses a system for providing network-based firewall policy configuration and facilitation, comprising:

- **A firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user's firewall policy** [See page 3, paragraph 5-7] (*By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Session controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service and this run-time session controls meets adding an application not currently supported by a user's firewall policy.) and*

- **To generate a time window during which a user can run the application**; [See table 4-1 on page 3 and 4, see common Run-time controls] (*These session controls are common to all network services. They define the basic elements of any session, such as **its time of day**, date, User ID, Host ID, and type of service. These controls are defined using security policies.) and*

- **A policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a firewall modification request from the firewall facilitation**

coordinator [See page 3, paragraph 5-7 and see also table 4-1 on page 3 and 4, see common Run-time controls] (By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service. These session controls are common to all network services. They define the basic elements of any session, such as its time of day, date, User ID, Host ID, and type of service. These controls are defined using security policies)

determine whether the application includes one or more questionable packets, [See page 9](On page 9 Cisco discloses, how the Cisco Centri Firewall enforces security policies, identifies and defines the major components of the architecture, and explains how **it prevents common attacks through detailed evaluation of network packets and intelligent countermeasures**, meets the limitation recited as “determine whether the application includes one or more questionable packets.” Because if the firewall has the capability of preventing common attacks through detailed evaluation of network packets and intelligent countermeasures then it implies that it has also the capability of determining whether the application includes one or more questionable packets/attacking packets) **and**

to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more

questionable packets. [Page 3, third paragraph and page 3, 6-7 paragraph]

(For instance applicant's published specification on paragraph 0048 discloses the following in support of this limitation.

*"If the blocking history is completely acceptable i.e., the PMA finds no questionable packets, at 520, the user's firewall policy **is modified by adding new rules allowing the passage of the new application's packet types to the set of firewall policy rules. Optionally in some cases, it may be possible to modify existing rules rather than adding new rules, depending on the specifics of the rules and their parameters. The firewall policy rules are preferably formed from the pertinent aspects of the identified packets, such as the source and destination addresses, source and destination ports numbers, whether TCP or UDP packets, or other protocol numbers, etc."*** The reference on the record also discloses the same concept. For instance, Cisco on page 3, third paragraph discloses, that Centri Firewall filters session attempts according to the rules defined in a security policy. A security policy specifies which network objects are allowed to communicate with each other, and each security policy is designed to enforce some part of the overall network security policy defined by an organization. You can specify which internal network objects can communicate with which external network objects and vice versa. Other options exist by which you can filter communications, **such as time of day, destination, and type of protocol being used to conduct the communication.** Furthermore, Cisco on page 3, paragraph 6 and 7, discloses Session control and Run-time session controls which are capable of determining whether the application includes one or more questionable packets at the run time. For instance, under the session control, the following has been disclosed. "Session controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed

during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static and Run-time session controls **are those session controls that can be modified at the time the session request is received by the firewall.** Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service.” And this meets the limitation recited as “to modify the user’s firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets.”)

Furthermore,

Referring to the pervious Independent claims 48, 50 and 52,

The references on the record namely the combination of **Cisco and Yoshihara**, discloses each and every limitations recited in the previous independent claims **48, 50 and 52** before the claims were amended.

For instance, referring to the previous independent 48, 50 and

52 **Cisco**, the primary reference on the record, discloses a system for providing network-based **firewall** policy configuration and facilitation, comprising:

- **A firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user’s firewall policy** [See page 3, paragraph 5-7] (“By By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is

transferred during that session. Session controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service and this run-time session controls meets adding an application not currently supported by a user's firewall policy.) and

- **To generate a time window during which a user can run the application; [See table 4-1 on page 3 and 4, see common Run-time controls]**
*(These session controls are common to all network services. They define the basic elements of any session, such as **its time of day**, date, User ID, Host ID, and type of service. These controls are defined using security policies.) and*
- **A policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a firewall modification request from the firewall facilitation coordinator [See page 3, paragraph 5-7 and see also table 4-1 on page 3 and 4, see common Run-time controls] (By evaluating incoming requests to start a new session against the session controls and responses defined in a security policy, Cisco Centri Firewall can determine whether to allow that session. If it does allow a session, Cisco Centri Firewall also determines how to modify the data that is transferred during that session. Run-time session controls are those session controls that can be modified at the time the session request is received by the firewall. Run-time session controls are defined using security policies and can either apply to all communications or to a specific network service. These session controls are common to all network services. They define the basic elements of**

any session, such as its time of day, date, User ID, Host ID, and type of service.

These controls are defined using security policies)

determine whether the application includes one or more questionable packets, [See page 9](On page 9 Cisco discloses, how the Cisco Centri Firewall enforces security policies, identifies and defines the major components of the architecture, and explains how **it prevents common attacks through detailed evaluation of network packets and intelligent countermeasures, meets the limitation recited as “determine whether the application includes one or more questionable packets.” Because if the firewall has the capability of preventing common attacks through detailed evaluation of network packets and intelligent countermeasures then it implies that it has also the capability of determining whether the application includes one or more questionable packets/attacking packets) and**

to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets. [Page 3, third paragraph and page 3, 6-7 paragraph]
(For instance applicant's published specification on paragraph 0048 discloses the following in support of this limitation.

*“If the blocking history is completely acceptable i.e., the PMA finds no questionable packets, at 520, the user's firewall policy **is modified by adding new rules allowing the passage of the new application's packet types to the set of firewall policy rules. Optionally in some cases, it may be possible to modify existing rules rather than adding new rules, depending on the specifics of the rules and their parameters. The firewall policy rules are preferably formed from the pertinent aspects of the identified packets,***

such as the source and destination addresses, source and destination ports numbers, whether TCP or UDP packets, or other protocol numbers, etc.” The reference on the record also discloses the same concept. For instance, Cisco on page 3, third paragraph discloses, that Centri Firewall filters session attempts according to the rules defined in a security policy. A security policy specifies which network objects are allowed to communicate with each other, and each security policy is designed to enforce some part of the overall network security policy defined by an organization. You can specify which internal network objects can communicate with which external network objects and vice versa. Other options exist by which you can filter communications, **such as time of day, destination, and type of protocol being used to conduct the communication.** Furthermore, Cisco on page 3, paragraph 6 and 7, discloses Session control and Run-time session controls which are capable of determining whether the application includes one or more questionable packets at the run time. For instance, under the session control, the following has been disclosed. “Session controls are predominately specific to a network service and are used to act upon a session to provide stricter control over what is and what is not allowed during that session. Within Cisco Centri Firewall, two types of session controls exist: run-time and static and Run-time session controls **are those session controls that can be modified at the time the session request is received by the firewall.** Run-time session **controls are defined using security policies and can either apply to all communications or to a specific network service.”** And this meets the limitation recited as “to modify the user's firewall policy to allow at least a portion of the packets associated with the application to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets.”)

Cisco does not explicitly teach wherein the policy modification agent is further configured to group the types of questionable packets singly and in combination of two or more, and to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

However, in the same field of endeavor, **Yoshihara on paragraph 0034 discloses the following,**

“Counters 3113 to 3117 count the number of passing IP packets or the number of IP packet bytes. An unconditional dropper 3107 discards a packet unconditionally. Selective droppers 3108, 3109, and 3110 **discards selectively a packet under a predetermined condition.** Queues 3118 to 3121 queue an input IP packet. A scheduler 3130 reads out packets from such queues 3118 to 3121 **each in accordance with a predetermined sequence and priority,** and outputs them to an output I/F 36.” Furthermore, on paragraph 0100, Yoshihara discloses the following, “the present invention is similarly applicable **to policy based network management employing a firewall for making customized access control for each user, company, host, terminal, and application**” and this meets the limitation recited as, “the policy modification agent is further configured to group the types **of questionable packets** singly and in combination of two or more, and **to prioritize** the groups based on a likelihood that the groups **will be required to be added to the firewall policy** in order to allow the new application to function properly, and to label **the groups in order of priority.**”

However, as applicant's representative persuasively argued neither Cisco nor **Yoshihara alone or in combination teaches the new limitation recited in the respective independent claims.**

None of the prior art of record taken singularly or in combination teaches a method for providing network-based firewall policy configuration and facilitation associated with the firewall, with the new functional limitation added to the respective independent claims together with the limitation recited in the former independent claims. For this reason, **independent claims 1, 16, 31, 48, 50 and 52 are found to be novel and are allowed.**

7. The dependent claims which are dependent on the above **independent claims 1, 16, 31, 48, 50 and 52** being further limiting to the independent claim, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

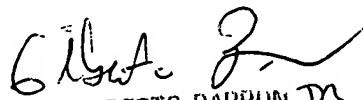
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L.
11/15/2007


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100